PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-229859
(43)Date of publication of application : 16.08.2002

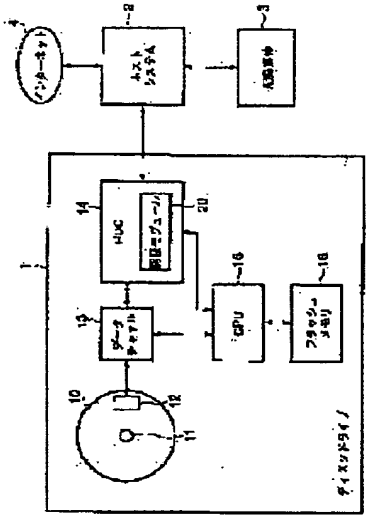
(51)Int.CL G06F 12/14
H04L 9/14
H04L 9/32

(21)Application number : 2001-023362
(22)Date of filing : 31.01.2001

(71)Applicant : TOSHIBA CORP
(72)Inventor : IGARI CHIKASHI

(54) DISK MEMORY AND AUTHENTICATING METHOD APPLIED THERETO

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a disk memory establishing a plurality of secret ranges and having a different authenticating function for each secret range.
SOLUTION: A disk 10 wherein a plurality of secret ranges is established is provided. An authentication module 20 allows only a host system 2 authenticated by the authenticating function to access to each secret range. By exchanging information with the host system 2, the authentication module 20 uses key information established for each secret range and range inherent information to conduct a certifying procedure for deciding whether access is permitted or not for each secret range.



LEGAL STATUS

[Date of request for examination] 13.12.2004
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－229859
（Ｐ2002－229859Ａ）
(43)公開日　平成14年８月16日(2002.8.16)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｅ	５Ｂ０１７
			３２０Ｂ	５Ｊ１０４
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１	
9/32			６７５Ａ	

審査請求　未請求　請求項の数９　ＯＬ　（全９頁）

(21)出願番号　特願2001－23362(Ｐ2001－23362)

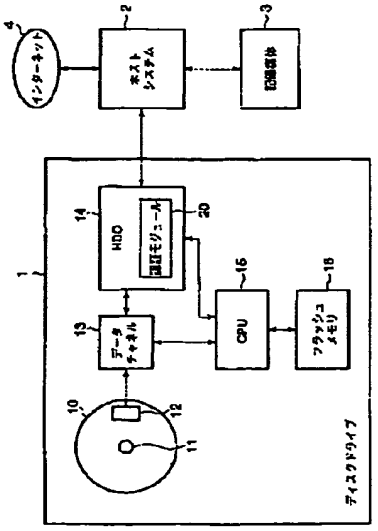
(22)出願日　平成13年１月31日(2001.1.31)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　猪狩　史
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5B017 AA06 BA07 BA09 CA05 CA07
5J104 AA07 AA13 KA02 KA04 NA02
NA27 NA35 PA07

(54)【発明の名称】　ディスク記憶装置及び同装置に適用する認証方法

(57)【要約】
【課題】ディスク上に複数の秘匿領域を設定し、各秘匿領域毎に異なる認証機能を有するディスク記憶装置を提供することにある。
【解決手段】複数の秘匿領域が設定されたディスク１０が設けられている。各秘匿領域は、認証モジュール２０により認証機能で認証されたホストシステム２のみによりアクセスが可能となる。認証モジュール２０はホストシステム２との情報交換により、各秘匿領域ごとに設定されている鍵情報と領域固有情報を使用して、各秘匿領域毎にアクセスを許可するか否かを決定するための認証手順を実行する。



1

【特許請求の範囲】

【請求項１】 複数の所定記憶領域を特別のアクセス条件を必要とする複数の秘匿領域として設定可能なディスク記憶媒体と、

前記各秘匿領域に対応する複数の鍵情報及び当該各秘匿領域に共通な固有情報を記憶している記憶手段と、

前記鍵情報と前記固有情報とから生成される前記各秘匿領域毎の領域固有情報を使用して、当該各秘匿領域毎にアクセスを許可するか否かを決定するための認証処理を実行する認証手段とを具備したことを特徴とするディスク記憶装置。

【請求項２】 前記認証手段は、

乱数とアクセス対象の秘匿領域に対応する領域固有情報とを使用して所定の暗号化演算処理を実行する暗号化手段と、

当該秘匿領域のアクセスを要求する外部装置に対して前記鍵情報及び前記固有情報を送出する手段と、

前記外部装置から前記乱数及び前記領域固有情報に相当する各情報を使用した暗号化演算結果を受信し、当該暗号化演算結果と前記暗号化手段による暗号化演算結果とが一致した場合に、アクセス対象の秘匿領域に対するアクセスを許可する判定手段とを有することを特徴とする請求項１記載のディスク記憶装置。

【請求項３】 前記認証手段は、

乱数又は疑似乱数を生成する乱数生成手段を有し、

当該乱数生成手段により生成した乱数を前記暗号化手段に与えると共に、前記外部装置に送出する手段とを有することを特徴とする請求項２記載のディスク記憶装置。

【請求項４】 前記認証手段は、

指定の秘匿領域のアクセスを要求する外部装置に対して当該秘匿領域に対応する鍵情報及び前記固有情報を送出する手段と、

前記外部装置から供給された乱数と、アクセス対象の秘匿領域に対応する領域固有情報とを使用して所定の暗号化演算処理を実行する暗号化手段と、

前記外部装置から、前記鍵情報及び前記固有情報を使用して得られた前記領域固有情報に相当する情報と前記乱数とを使用した暗号化演算結果を受信する手段と、

前記外部装置からの暗号化演算結果と前記暗号化手段による暗号化演算結果とが一致した場合に、アクセス対象の秘匿領域に対するアクセスを許可する判定手段とを有することを特徴とする請求項１記載のディスク記憶装置。

【請求項５】 前記認証手段は、

乱数とアクセス対象の秘匿領域に対応する領域固有情報とを使用して所定の暗号化演算処理を実行する暗号化手段と、

当該秘匿領域のアクセスを要求する外部装置に対して前記鍵情報及び前記固有情報を送出する手段とを有し、

前記外部装置において前記乱数及び前記領域固有情報に

2

相当する各情報を使用した暗号化演算結果と、前記暗号化手段による暗号化演算結果とを比較する認証処理で両者の演算結果が一致した場合に、各秘匿領域毎にアクセスを許可するか否かを決定するための前記認証処理を実行するように構成されていることを特徴とする請求項１記載のディスク記憶装置。

【請求項６】 前記各秘匿領域毎の領域固有情報を記憶する手段と、

外部装置からの更新要求に応じて前記鍵情報と前記領域固有情報を更新する更新手段とを特徴とする請求項１から請求項５のいずれか記載のディスク記憶装置。

【請求項７】 複数の所定記憶領域を特別のアクセス条件を必要とする複数の秘匿領域として設定可能なディスク記憶媒体と、前記各秘匿領域に対応する複数の鍵情報及び当該各秘匿領域に共通な固有情報を記憶している記憶手段とを有するディスク記憶装置に適用する認証方法であって、

ホストシステムによりアクセス対象として指定される秘匿領域毎に、前記記憶手段から当該秘匿領域に対応する前記鍵情報及び前記固有情報を読出すステップと、

前記鍵情報及び前記固有情報を使用して当該秘匿領域に対応する領域固有情報を生成するステップと、

前記領域固有情報を使用して、当該秘匿領域のアクセスを許可するか否かを決定するステップと、から構成されることを特徴とする認証方法。

【請求項８】 前記ホストシステムに対して前記鍵情報及び前記固有情報を送出するステップと、

乱数と当該秘匿領域に対応する領域固有情報とを使用して所定の暗号化演算処理を実行するステップと、

前記ホストシステムから前記乱数及び前記領域固有情報に相当する各情報を使用した暗号化演算結果を受信するステップと、

前記ホストシステムからの暗号化演算結果と、前記暗号化演算処理ステップにより算出された暗号化演算結果とが一致した場合に、アクセス対象の秘匿領域に対するアクセスを許可するステップとを有することを特徴とする請求項７記載のディスク記憶装置。

【請求項９】 複数の所定記憶領域を特別のアクセス条件を必要とする複数の秘匿領域として設定可能なディスク記憶媒体と、前記各秘匿領域に対応する複数の鍵情報、当該各秘匿領域毎の領域固有情報、及び複数種の暗号化・復号化機能に関する機能情報を記憶している記憶手段とを有するディスク記憶装置に適用する認証方法であって、

ホストシステムにより指定された機能情報を前記記憶手段から読出して、当該ホストシステムに送出するステップと、

前記送出ステップにより送出した機能情報に基づいて、前記ホストシステムにより構成された鍵情報を前記ホストシステムから受信するステップと、

前記受信ステップにより受信した鍵情報を使用して、前記ホストシステムにより指定された秘匿領域に対応する領域固有情報を生成するステップと、

前記受信ステップにより受信した鍵情報及び前記生成ステップにより生成した領域固有情報を使用して、前記ホストシステムにより指定された秘匿領域に対する鍵情報及び領域固有情報を更新するステップと、から構成されることを特徴とする認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えばハードディスクドライブに適用し、特にディスク上の秘匿領域に対するアクセスを制限するための認証機能を備えたディスク記憶装置に関する。

【０００２】

【従来の技術】近年、インターネットやディジタル放送網などから、画像（動画及び静止画）や音声などのコンテンツデータ、またはプログラムを配信する情報サービスのシステムが注目されている。このようなシステムでは、配信されるデータは、パーソナルコンピュータなどを含むディジタル機器などにダウンロードされて、当該機器に装着されている記録媒体に保存される。ディジタル機器には、ディジタルテレビジョン装置や、携帯電話または専用再生機器などのモバイル情報機器が含まれる。

【０００３】これらの機器に装着されている記録媒体は、フラッシュＥＥＰＲＯＭなどからなるメモリカードや、ハードディスクドライブ（ＨＤＤ）又は光磁気ディスクドライブ（ＭＯ）などのディスクドライブからなる。

【０００４】ところで、情報サービスシステムでは、コンテンツデータやプログラムの著作権保護のために、特にコピー防止を目的とするセキュリティ機能が必要不可欠な要素になっている。このセキュリティ機能には、記録媒体の一部の記憶領域を秘匿領域として設定し、当該秘匿領域のアクセス時に認証処理を実行する認証機能が含まれる。認証機能は、当該秘匿領域に対するアクセス要求がある場合に、アクセスを許可するか否かを判定する認証手順からなる。

【０００５】

【発明が解決しようとする課題】従来では、例えばフラッシュＥＥＰＲＯＭからなるメモリカードを使用するシステムに対しては、各種の認証機能が開発されている。これに対して、ＨＤＤを代表とするディスクドライブを使用するシステムでは、ホストシステム（ディジタル機器の本体）側の認証機能としては各種の方式があるが、ドライブ自体には制限された認証機能しか設けられていない。

【０００６】ディスクドライブの認証機能としては、ディスク上の所定の記憶領域を秘匿領域として設定し、当該秘匿領域に対するアクセスを制限するための認証手順が提案されている。秘匿領域には、例えば暗号化／復号化処理に必要な鍵情報が格納される。この鍵情報を使用して、非秘匿領域（通常記憶領域）に格納されたコンテンツデータの暗号化又は復号化を行なう機能が実現される。

【０００７】従来の認証機能は、１種類の認証手順により秘匿領域に対するアクセスの許可を判定する方式が一般的である。メモリカードなどでは、記憶容量が制限されているため、秘匿領域も制限される。従って、通常では１種類の認証手順による認証機能が設定されている。しかしながら、ディスクドライブでは、相対的に大容量であるため、ディスク上に複数の秘匿領域を設定することが可能である。この場合、各秘匿領域毎に異なる認証機能を設定することが可能であれば、応用範囲の広いシステムを実現することが可能となる。

【０００８】そこで、本発明の目的は、ディスク上に複数の秘匿領域を設定し、各秘匿領域毎に異なる認証機能を設定できるディスク記憶装置を提供することにある。

【０００９】

【課題を解決するための手段】本発明は、記録媒体であるディスク上に、アクセスが制限されている複数の秘匿領域を設定し、各秘匿領域毎に異なる認証機能により認証処理を実行するディスクドライブに関する。

【００１０】即ち、本ディスクドライブは、複数の所定記憶領域を特別のアクセス条件を必要とする複数の秘匿領域として設定可能なディスク記憶媒体と、各秘匿領域に対応する複数の鍵情報及び当該各秘匿領域に共通な固有情報を記憶している記憶手段と、鍵情報と固有情報とから生成される各秘匿領域毎の領域固有情報を使用して、当該各秘匿領域毎にアクセスを許可するか否かを決定するための認証処理を実行する認証手段とを有する。

【００１１】具体的には、ディスクドライブは、暗号化・復号化機能を実行する暗号化回路を例えばディスクコントローラの内部に備えている。また、ディスクドライブは、ドライブ自体を識別するためのドライブの固有情報（ＩＤ情報）を、例えばドライブ内のフラッシュＥＥＰＲＯＭに記憶している。各秘匿領域毎に設定された各鍵情報は、例えばディスク上の秘匿領域又はフラッシュＥＥＰＲＯＭに記憶されている。

【００１２】複数の秘匿領域には、例えば非秘匿領域に格納されて、暗号化されたコンテンツデータ（例えば暗号化された音楽データ）をアクセスするための（復号化）鍵情報が保存される。この場合、各秘匿領域ごとに、異なる暗号化・復号化方式に対応する鍵情報や、またはコンテンツの種類毎に異なる鍵情報を保存することが可能である。従って、本発明のディスクドライブを使用したシステムであれば、暗号化・復号化方式の異なるコンテンツデータを保存した場合に、当該各コンテンツデータを復号化するための各鍵情報を、秘匿領域のいず

れから得ることが可能である。本発明では、各秘匿領域に対するアクセスを実行する場合に、各秘匿領域毎に異なる認証手順での認証処理が実行される。従って、複数種の暗号化・復号化方式を適用した情報に対する情報保護機能を実現したシステムを提供することが可能となる。

【００１３】本発明の具体的適用分野としては、例えばパーソナルコンピュータやモバイル情報機器の交換型記憶装置として使用するためのカード型（又はモバイル型）ディスクドライブや、インターネットやＬＡＮなどに使用されるサーバ用ストレージ装置である。

【００１４】本発明の別の観点としては、各秘匿領域に対応する鍵情報及び領域固有情報を更新する更新機能を有するディスクドライブである。この更新機能は、ホストシステムにより指定された秘匿領域に対応する鍵情報を、ディスクドライブが予め保存している暗号化・復号化機能情報に基づいてホストシステムにより構成された鍵情報に更新する機能である。ディスクドライブは、予め複数種の方式の暗号化・復号化プログラムを記憶している。暗号化・復号化機能情報は、当該暗号化・復号化プログラムのプログラム名または暗号化・復号化の方式名を示す情報である。

【００１５】ディスクドライブは、該当する鍵情報を更新すると、当該鍵情報から領域固有情報を算出して、ホストシステムにより指定された秘匿領域に対応する領域固有情報を更新する。従って、暗号化・復号化方式の変更に伴って、該当する秘匿領域（暗号化・復号化処理に必要な鍵情報を保存する）に対して、認証手順を変更することが可能となる。

【００１６】

【発明の実施の形態】以下図面を参照して、本発明の実施の形態を説明する。

【００１７】（ディスクドライブの構成）同実施形態では、ＨＤＤであるディスクドライブ１と、ホストシステム２とを有するディジタル機器を想定し、ディスクドライブ１はホストシステム２からのコマンドに応じて各種の動作を実行する。

【００１８】ホストシステム２は、マイクロプロセッサと各種アプリケーション・ソフトウェアとをメイン要素とし、インターネット４やディジタル放送ネットワークに接続している。ホストシステム２は、当該ネットワーク（インターネット４を含む）から配信されたコンテンツデータ（例えば音楽データや画像データなど）やプログラムを、ディスクドライブ１にダウンロードする機能を有する。さらに、ホストシステム２は、ダウンロードした配信データ（暗号化データ）の復号化機能やコピー防止機能などのセキュリティ機能を備えている。また、ホストシステム２は、ディスクドライブ１から読出したコンテンツデータまたはインターネット４から配信されたコンテンツデータを、例えばメモリカードなどの記録

媒体３にコピーする機能を有する。この記録媒体３は、例えば携帯型再生機器（モバイル情報機器）の交換型記録媒体として使用される。

【００１９】ディスクドライブ１は、記録媒体としてのディスク１０と、データの記録又は再生を行なうヘッド１２と、データチャネル１３と、ディスクコントローラ（ＨＤＣ）１４と、ＣＰＵ１５と、フラッシュＥＥＰＲＯＭ（フラッシュメモリ）１６とを有する。また、フラッシュメモリ１６以外に、ＲＡＭ及びＲＯＭなどのメモリも設けられている。

【００２０】ディスク１０は、データ記録再生時には、ＣＰＵ１５の制御によりスピンドルモータ１１により高速回転している。ヘッド１２は、ＣＰＵ１５の制御に基づいて、図示しないヘッドアクチュエータによりディスク１０の半径方向に移動可能に構成されている。データチャネル１３は、ヘッド１２からのリード信号を再生データに変換し、ディスクコントローラ１４からの記録データを記録信号に変換するための信号処理を行なうリード／ライト回路である。

【００２１】ＨＤＣ１４は、ディスクドライブ１とホストシステム２とのインターフェース（例えばＡＴＡインターフェース仕様）を構成し、ホストシステム２からの各種のコマンド及びデータの転送を制御する。ＨＤＣ１４は、同実施形態の認証機能に関係する認証モジュール２０を有する。認証モジュール２０は、専用ＬＳＩからなるハードウエアである。具体的には、認証モジュール２０は、図６に示すように、暗号化・復号化回路２００、乱数発生回路２０１、及び暗号化・復号化処理に必要な鍵データなどを格納するフラッシュＥＥＰＲＯＭ２０２等を備えている。暗号化・復号化回路２００は、後述するように、複数種の方式（Ａ～Ｃ）の暗号化・復号化機能部を有する。また、暗号化・復号化回路２００は、複数種の方式（Ａ～Ｃ）の暗号化・復号化プログラムを記憶し、ＣＰＵ１５に当該プログラムを供給する構成でもよい。この場合には、ＣＰＵ１５は、暗号化・復号化プログラムを実行して、同実施形態に関する認証処理や、暗号化・復号化処理を実行する。

【００２２】ＣＰＵ１５は、ドライブ１のメイン制御要素であり、データ記録再生動作及びヘッド位置決め制御などの他に、同実施形態に関係する認証機能に関係する制御動作を実行する。フラッシュメモリ１６は、図３に示すように、認証機能に必要なドライブ１の固有情報（ドライブＩＤ情報）１６０を格納するための不揮発性メモリである。また、フラッシュメモリ１６は、認証処理や暗号化・復号化処理に必要な鍵情報などを格納するメモリとして使用されてもよい。

【００２３】（ディスクの構成）同実施形態では、図２に示すように、ディスク１０上の所定記憶領域（例えば内周側エリア）は、複数の秘匿領域１０１～１０３（ここでは３領域とする）が設定される。各秘匿領域１０１

～１０３は、例えばホストシステム２からの設定コマンドにより設定される特別の領域であり、アクセスが制限されている。ここで、ディスク１０上の全記憶領域から秘匿領域１０１～１０３を除いた非秘匿領域１００は、認証機能とは無関係な通常使用領域である。この通常使用領域１００には、コピー制限されているコンテンツデータ（配信データ）などが暗号化されて格納（ダウンロード）される。

【００２４】各秘匿領域１０１～１０３は、例えばインターネット４から非秘匿領域１００にダウンロードされた暗号化データ（コンテンツデータ）を復号化したり、または当該コンテンツデータを暗号化するために必要な鍵情報などを格納する。さらに、各秘匿領域１０１～１０３は、それぞれの領域のアクセスでの認証処理に必要な鍵情報１０１A～１０３Aを格納するためのエリア、及び後述する各領域固有情報１０１B～１０３Bを格納するためのエリアを有する。同実施形態の認証機能は、当該鍵情報１０１A～１０３A、各領域固有情報１０１B～１０３B及びフラッシュメモリ１６に格納されたドライブＩＤ情報１６０を使用する。

【００２５】（認証処理）以下主として図４及び図５のフローチャートを参照して、秘匿領域１０１～１０３のアクセスに対する認証手順を説明する。なお、図４及び図５のフローチャートでは、ディスクドライブ１の処理と、ホストシステム２の処理とが併記されており、点線は情報やコマンドの交換を意味している。

【００２６】ここでは、ホストシステム２が、ディスク１０の非秘匿領域１００から暗号化データ（例えば音楽データなどのコンテンツデータ）を復号化して、メモリカードなどの記録媒体３にコピーする場合を想定する。このため、ホストシステム２は、所定の秘匿領域（１０１とする）から当該コンテンツデータを復号化するための鍵情報を取得するため、ディスクドライブ１に対してアクセス要求を実行する。ディスクドライブ１は、当該アクセス要求に対して所定の認証処理を実行する。

【００２７】まず、ホストシステム２からドライブ１を識別するためのドライブＩＤ情報１６０の読出し要求がなされると、ドライブ１はフラッシュメモリ１６に格納された当該ドライブＩＤ情報１６０をホストシステム２に送出する（ステップＨ１，Ｄ１）。なお、ディスクドライブ１では、ホストシステム２とのデータや情報の転送は、ＨＤＣ１４及びＣＰＵ１５により実行される。

【００２８】次に、ホストシステム２は、アクセスすべき秘匿領域１０１を選択し、当該秘匿領域１０１に対する鍵情報１０１Ａの読出し要求を行なう（ステップＨ２，Ｈ３）。この要求に応じて、ドライブ１は、ディスク１０上の指定された秘匿領域１０１から鍵情報１０１Ａを読出して、ホストシステム２に送出する（ステップＤ２）。

【００２９】ホストシステム２は、読出したドライブＩＤ情報１６０と鍵情報１０１Ａとを所定の復号化機能部（暗号化・復号化プログラム）に与えて、当該秘匿領域１０１に対応する領域固有情報（１０１Ｂに相当する情報）を算出（復号化）する（ステップＨ４）。即ち、同実施形態の認証機能は、秘匿領域１０１に対応する領域固有情報１０１Ｂをドライブ１がホストシステム１に送出することなく、両者において共通の領域固有情報１０１Ｂを有する構成である。従って、秘匿領域１０１をアクセスするための認証手順に必要な領域固有情報１０１Ｂが、外部に漏洩することは無く、高いセキュリティ性を備えた認証機能である。

【００３０】さらに、ホストシステム２は、乱数発生機能部（乱数発生プログラム）から乱数（疑似乱数）を生成し、予め備えている暗号化機能部（暗号化プログラム）に当該乱数と、算出した領域固有情報とを与えて、暗号化情報（暗号化演算結果）を算出する（ステップＨ５，Ｈ６）。ホストシステム２は、生成した乱数をディスクドライブ１に送出する（ステップＨ７）。一方、ディスクドライブ１では、認証モジュール２０は、暗号化・復号化回路２００での所定の暗号化手順（例えばプログラムＡ）により、当該乱数と領域固有情報１０１Ｂとを使用して、暗号化演算を実行し、演算結果である暗号化情報を算出する（ステップＤ３）。ドライブ１は、算出した当該暗号化情報をホストシステム２に送出する（ステップＤ４）。

【００３１】ホストシステム２は、自身が算出した暗号化情報と、ドライブ１から得られた暗号化情報とを比較して、一致していれば両者の暗号化手順が同一であり、第１段階の認証処理は成功であると判定する（ステップＨ９のＹＥＳ）。一方、両者の暗号化情報が不一致の場合には、両者の暗号化手順が異なるため、認証処理は失敗となり、これ以後の手順は中止となる（ステップＨ９のＮＯ）。

【００３２】ホストシステム２での認証処理が成功すると、ディスクドライブ１での認証処理に移行する。以下図５のフローチャートを参照して、当該認証手順を説明する。

【００３３】まず、ホストシステム２からの乱数発生の要求に応じて、ドライブ１の認証モジュール２０は、乱数発生回路２０１により乱数（疑似乱数）を生成する（ステップＨ１０，Ｄ１０）。ドライブ１は、生成した乱数をホストシステム１に送出する。

【００３４】ホストシステム２は、ドライブ１から受信した乱数と、前の認証手順で算出した領域固有情報とを、暗号化機能部（暗号化プログラム）に与えて、暗号化情報（暗号化演算結果）を算出する（ステップＨ１１）。ホストシステム２は、算出した暗号化情報をディスクドライブ１に送出する。一方、ディスクドライブ１では、認証モジュール２０は、生成した乱数と領域固有情報１０１Ｂとを暗号化・復号化回路２００に与えて、

暗号化演算を実行し、演算結果である暗号化情報を算出する（ステップＤ１１）。

【００３５】認証モジュール２０は、自身が算出した暗号化情報と、ホストシステム２から得られた暗号化情報とを比較して、一致していれば認証処理が成功であると判定する（ステップＨ１２のＹＥＳ）。これにより、ディスクドライブ１は、ホストシステム２からの秘匿領域１０１に対するアクセス要求を許可し、当該秘匿領域１０１から読出した情報（復号化に必要な鍵情報）をホストシステム２に転送する。一方、両者の暗号化情報が不一致の場合には、認証モジュール２０は認証処理が失敗として判定する（ステップＨ１２のＮＯ）。この場合には、ホストシステム２からの秘匿領域１０１に対するアクセス要求は、認められない。

【００３６】以上のように同実施形態の認証手順により、ディスクドライブ１は、自身と同一方式の暗号化・復号化機能（暗号化・復号化プログラム）を備えているホストシステム２に対してのみ、秘匿領域に対するアクセスを許可する。この場合、秘匿領域に対応する領域固有情報の交換をすることなく、両者が有する暗号化・復号化機能（暗号化・復号化プログラム）の方式が同一であるか否かを判定する。従って、秘匿領域に対応する領域固有情報が外部に漏洩することなく、高いセキュリティ性を確保できる。なお、秘匿領域に対するアクセス許可は、１回のみとする制限を設けることが望ましい。さらに、ディスクドライブ１は、秘匿領域から読出した情報をホストシステム２に送出する場合に、認証手順で送出した乱数で暗号化した情報を送出することが、セキュリティの面で望ましい。

【００３７】また、ディスク１０上の秘匿領域１０１～１０３は、通常使用領域である非秘匿領域１００と比較して、認証処理を要するため、アクセス時間が増大する。そこで、秘匿領域１０１～１０３に格納する情報は、非秘匿領域１００に格納（ダウンロード）したコンテンツデータ（暗号化データ）の復号化に必要な鍵情報などに制限することが望ましい。

【００３８】（鍵情報と領域固有情報の更新処理）図７は、ディスク１０上の秘匿領域１０１～１０３に格納されている鍵情報１０１Ａ～１０３Ａ、及び領域固有情報１０１Ｂ～１０３Ｂを更新するときの手順を示すフローチャートである。

【００３９】まず、前述の認証手順により、ディスクドライブ１とホストシステム２間の認証処理を実行して、ホストシステム２は、ディスク１０上の指定された秘匿領域１０１に対してアクセスが可能であるとする（ステップＨ２０，Ｄ２０）。ホストシステム２は、ディスクドライブ１が有する暗号化・復号化機能に関する情報（暗号化機能情報とする）を要求する（ステップＨ２１）。この暗号化機能情報とは、認証モジュール２０が有する暗号化・復号化回路２００での暗号化・復号化機能の種類（方式）を示す情報であり、具体的には方式名又はプログラム名に相当する。

【００４０】ディスクドライブ１は、認証モジュール２０が有する暗号化・復号化機能の種類（方式）を示す暗号化機能情報をホストシステム２に送出する（ステップＤ２１）。ホストシステム２は、受信した暗号化機能情報から、ドライブ１が有する暗号化・復号化機能の方式（複数種類）を認識する。ホストシステム２は、それらの中で新たに設定する方式に対応する暗号化手順（システムが有する暗号化プログラム）で、新たな鍵情報（更新情報）を構成する（ステップＨ２２）。この新たな鍵情報は、ホストシステムが指定した秘匿領域１０１に対応する更新情報である。

【００４１】さらに、前述の認証手順による再度の認証処理が実行された後に、ホストシステム２は、新しく構成した鍵情報及びその暗号化手順（暗号化プログラム）を示す情報（方式名）をディスクドライブ１に送出する（ステップＨ２４）。ディスクドライブ１では、ホストシステム２から受信した鍵情報を仮情報として、ディスク１０上の所定領域またはフラッシュメモリ１６に格納する（ステップＤ２３）。また、ホストシステムから指定された方式の暗号化手順（暗号化プログラム）を示す情報もディスク１０上の所定領域またはフラッシュメモリ１６に格納する。

【００４２】ディスクドライブ１では、ホストシステムからの情報で指定された方式の暗号化手順で、ホストシステムから与えられた新しい鍵情報とドライブＩＤ情報とを使用して、秘匿領域１０１に対応する仮の領域固有情報を算出する（ステップＤ２４）。具体的には、認証モジュール２０の暗号化・復号化回路２００は、ホストシステムからの情報で指定された方式の暗号化手順で、仮の領域固有情報を算出する暗号化演算を実行する。

【００４３】次に、ホストシステム２とディスクドライブ１とは、前述の認証手順を実行する（ステップＨ２５，Ｄ２５）。但し、この認証手順で使用される鍵情報及び領域固有情報は、いずれも更新された仮の鍵情報及び仮の領域固有情報である。また、暗号化手順（方式）は、ホストシステム２から指定されたものである。この認証手順により、ディスクドライブ１からの暗号化情報と、ホストシステム ２からの暗号化情報とが一致した場合には、認証処理は成功となる。従って、ホストシステム２とディスクドライブ１との間で、指定された秘匿領域１０１に対する鍵情報と領域固有情報の更新が確認されたことになる。

【００４４】ホストシステム２は、ディスクドライブ１に対して、新たな鍵情報と領域固有情報の更新を要求する（ステップＨ２６）。これにより、ディスクドライブ１は、仮の鍵情報及び仮の領域固有情報をそれぞれ更新情報として、正式に所定領域（秘匿領域１０１に確保されたエリア）に登録する（ステップＤ２６）。また、認

証モジュール２０は、ホストシステム２から指定された方式の暗号化手順（暗号化プログラム）を暗号化・復号化回路２００に設定することになる。

【００４５】以上のような更新機能により、初期時に設定されている秘匿領域１０１～１０３に対応する鍵情報１０１Ａ～１０３Ａ及び領域固有情報１０１Ｂ～１０３Ｂを、更新することができる。従って、ディスク１０上の秘匿領域に対して、高度のセキュリティを確保することが可能となる。なお、秘匿領域をディスクドライブの製品出荷時の初期状態に戻す機能を用意しておくことが望ましい。この場合、鍵情報及び領域固有情報も初期状態に戻すことになるが、セキュリティの面から、秘匿領域に格納されている情報を、初期状態に戻すときに消去することが望ましい。

【００４６】なお、同実施形態において、秘匿領域に対応する鍵情報１０１Ａ～１０３Ａ及び領域固有情報１０１Ｂ～１０３Ｂは、ディスク１０上に格納されている場合を想定したが、これに限ることなく、フラッシュメモリ１６に格納されている構成でもよい。また、認証モジュール２０は、暗号化・復号化機能を実行する回路２００を有し、当該回路２００内で複数方式の暗号化・復号化手順を設定できる用に構成されている。しかし、内部のフラッシュメモリ２０２に複数方式の暗号化・復号化手順が格納されており、回路２００は選択された暗号化・復号化手順で暗号化・復号化処理を実行する構成でもよい。また、同実施形態は、ハードウェアで構成された認証モジュール２０を想定したが、ＣＰＵ１５がフラッシュメモリ１６に格納されたプログラムにより、同実施形態の認証処理及び更新処理を実行する構成でもよい。

【００４７】

【発明の効果】以上詳述したように本発明によれば、ディスク上に複数の秘匿領域を設定し、各秘匿領域毎に異なる認証機能を有するディスク記憶装置を提供することができる。このようなディスク記憶装置であれば、各秘匿領域ごとに、異なる暗号化・復号化方式に対応する鍵情報や、またはコンテンツの種類毎に異なる鍵情報を保存することが可能である。これにより、高度のセキュリティを確保できる暗号化・復号化方式を適用したシステムを実現することが可能となる。また、各秘匿領域に対応する鍵情報及び領域固有情報を更新する更新機能を実現することにより、秘匿領域に対するセキュリティ性を向上することができる。

【００４８】本発明の具体的適用分野としては、例えばパーソナルコンピュータやモバイル情報機器の交換型記憶装置として使用するためのカード型（又はモバイル型）ディスクドライブや、インターネットやＬＡＮなどに使用されるサーバ用ストレージ装置である。

【図面の簡単な説明】

【図１】本発明の実施形態に関係するディスクドライブの要部を示すブロック図。

【図２】同実施形態に関するディスク上の記憶領域の構成を示す図。

【図３】同実施形態に関するフラッシュメモリの格納内容を示す図。

【図４】同実施形態に関する認証手順を説明するためのフローチャート。

【図５】同実施形態に関する認証手順を説明するためのフローチャート。

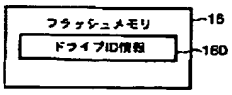
【図６】同実施形態に関する認証モジュールの内部構成を示すブロック図。

【図７】同実施形態に関する認証機能に含まれる情報更新手順を説明するためのフローチャート。

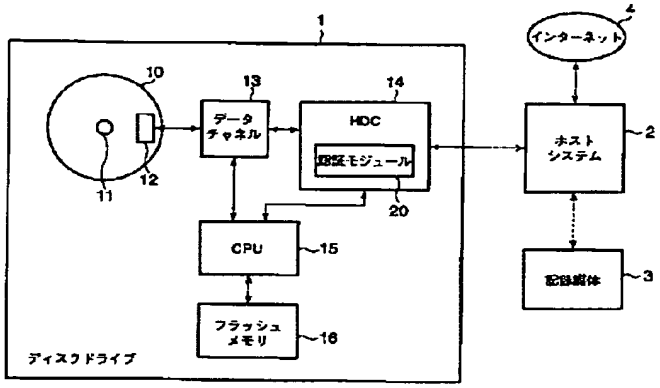
【符号の説明】

１…ディスクドライブ
２…ホストシステム
３…記録媒体（メモリカード）
４…インターネット
１０…ディスク
１１…スピンドルモータ
１２…ヘッド
１３…データチャネル
１４…ディスクコントローラ
１５…ＣＰＵ
１６…フラッシュメモリ
２０…認証モジュール
１０１～１０３…秘匿領域

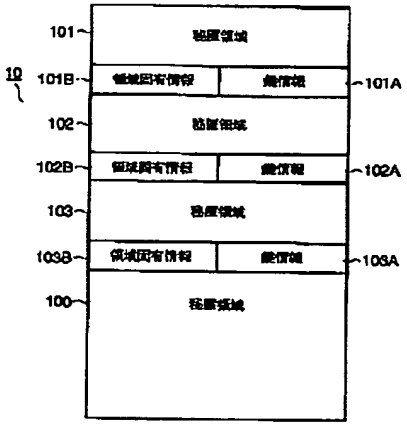
【図３】



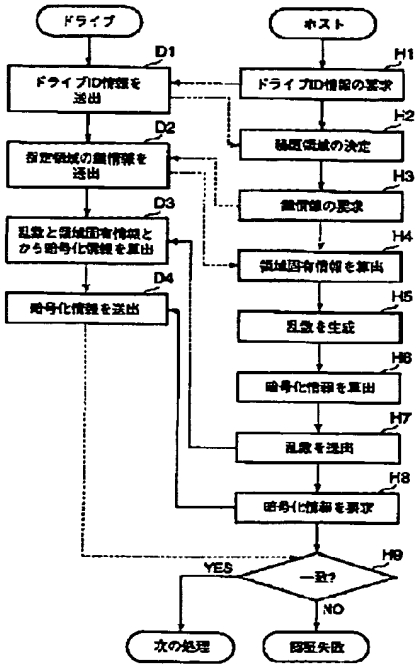
【図１】


1
インターネット
4
10
13
14
データ
チャネル
HDC
認証モジュール
ホスト
システム
2
12
11
20
CPU
15
記録媒体
3
フラッシュ
メモリ
16
ディスクドライブ

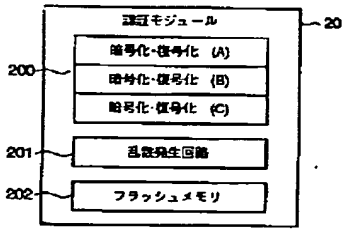
【図２】


101
10
101B
101A
102
102B
102A
103
103B
103A
100

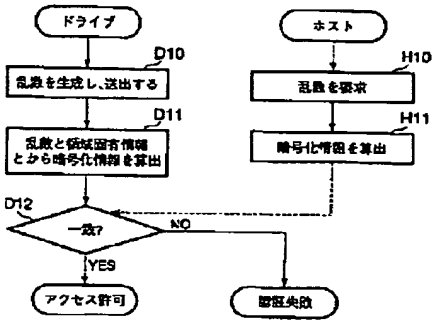
【図４】


ドライブ
ホスト
D1
H1
D2
H2
D3
H3
D4
H4
H5
H6
H7
H8
H9
YES
NO
一致?
次の処理

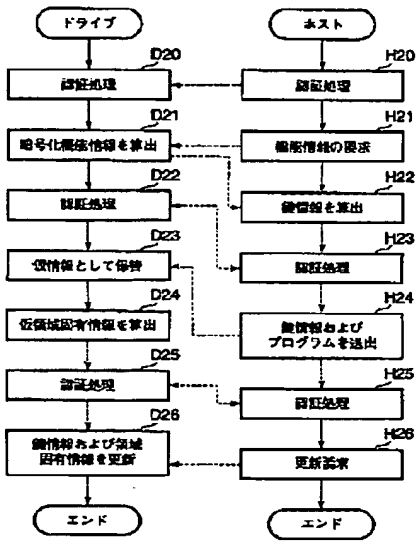
【図５】


認証モジュール
20
200
暗号化・復号化 (A)
暗号化・復号化 (B)
暗号化・復号化 (C)
201
乱数発生回路
202
フラッシュメモリ

【図５】


ドライブ
ホスト
D10
乱数を生成し、送出する
H10
乱数を要求
D11
乱数と領域固有情報とから暗号化情報を算出
H11
暗号化情報を算出
D12
一致?
NO
YES
アクセス許可
認証失敗

【図７】


ドライブ
ホスト
D20
認証処理
H20
認証処理
D21
暗号化機能情報を算出
H21
機能情報の要求
D22
認証処理
H22
鍵情報を算出
D23
仮情報として保持
H23
認証処理
D24
仮領域固有情報を算出
H24
鍵情報およびプログラムを送出
D25
認証処理
H25
認証処理
D26
鍵情報および領域固有情報を更新
H26
更新要求
エンド
エンド